ProCurve
Networking by HP

Release Notes:
Version U.11.04 Software
for the ProCurve 2510-48 Switches

Release U.11.04 supports these switches:

■ ProCurve Switch 2510-48 (J9020A)

These release notes include information on the following:

Applicable Product

ProCurve Switch 2510-48   (J9020A)

Trademark Credits

Microsoft®, Windows®, and Windows NT® are US
registered trademarks of Microsoft Corporation.
Adobe® and Acrobat® are trademarks of Adobe Systems
Incorporated. Java™ is a US trademark of Sun
Microsystems, Inc.

Software Credits

SSH on ProCurve Switches is based on the OpenSSH soft-
ware toolkit. This product includes software developed by
the OpenSSH Project for use in the OpenSSH Toolkit. For
more information on OpenSSH, visit

   http:// www.openssh.com.

SSL on ProCurve Switches is based on the OpenSSL soft-
ware toolkit. This product includes software developed by
the OpenSSL Project for use in the OpenSSL Toolkit. For
more information on OpenSSL, visit

   http://www.openssl.org.

This product includes cryptographic software written by
Eric Young (eay@cryptsoft.com). This product includes
software written by Tim Hudson (tjh@cryptsoft.com)

Contents

Software Management

Software Updates

Check the ProCurve Networking Web site frequently for free software updates for the various ProCurve switches you may have in your network.

Downloading Switch Documentation and Software from the Web

You can download software updates and the corresponding product documentation from HP's ProCurve web site as described below.

To Download a Software Version:

1. Go to the ProCurve Networking Web site at:

    http://www.procurve.com.

2. Click on **Software updates** (in the sidebar).

3. Under **Latest software**, click on **Switches**.

To Download Product Documentation: You will need the Adobe® Acrobat® Reader to view, print, and/or copy the product documentation.

1. Go to HP's ProCurve web site at **http://www.procurve.com**.

2. Click on **Technical support**, then **Product manuals**.

3. Click on the name of the product for which you want documentation.

4. On the resulting web page, double-click on a document you want.

5. When the document file opens, click on the disk icon in the Acrobat® toolbar and save a copy of the file.

Downloading Software to the Switch

The startup-config file generated by the latest software release may not be backward-compatible with the same file generated by earlier software releases.

HP periodically provides switch software updates through the ProCurve Networking Web site **http://www.procurve.com**). After you acquire the new software file, you can use one of the following methods for downloading it to the switch:

■ For a TFTP transfer from a server, do either of the following:

  • Click on **Download OS** in the Main Menu of the switch's menu interface and use the (default) **TFTP** option.

  • Use the **copy tftp** command in the switch's CLI (see below).

■ For an Xmodem transfer from a PC or Unix workstation, do either of the following:

  • Click on **Download OS** in the Main Menu of the switch's menu interface and select the **Xmodem** option.

  • Use the copy xmodem command in the switch's CLI (page 4).

■ Use the download utility in ProCurve Manager Plus.

■ A switch-to-switch file transfer

N o t e

Downloading new software does not change the current switch configuration. The switch configuration is contained in a separate file that can also be transferred, for example, for archive purposes or to be used in another switch of the same model.

This section describes how to use the CLI to download software to the switch. You can also use the menu interface for software downloads.

TFTP Download from a Server

Syntax: **copy tftp flash <ip-address> <remote-os-file> [< primary | secondary >]**

Note that if you do not specify the flash destination, the TFTP download defaults to the primary flash.

For example, to download a software file named R_11_04.swi from a TFTP server with the IP address of 10.28.227.103:

1. Execute the copy command as shown below:

   ```
   ProCurve # copy tftp flash 10.28.227.103 R_11_04.swi
   The primary OS image will be deleted. continue [y/n]? Y
   03125K
   ```

2. When the switch finishes downloading the software file from the server, it displays the progress message:

   ```
    Validating and Writing System Software to FLASH.
   ```

   When the CLI prompt re-appears, the switch is ready to reboot to activate the downloaded software

3. Reboot the switch.

   After the switch reboots, it displays the CLI or Main Menu, depending on the **Logon Default** setting last configured in the menu's Switch Setup screen.

Xmodem Download From a PC or Unix Workstation

This procedure assumes that:

■ The switch is connected via the Console RS-232 port on a PC operating as a terminal. (Refer to the Installation Guide you received with the switch for information on connecting a PC as a terminal and running the switch console interface.)

■ The switch software is stored on a disk drive in the PC.

■ The terminal emulator you are using includes the Xmodem binary transfer feature. (For example, in the Microsoft Windows NT® terminal emulator, you would use the **Send File** option in the **T**ransfer drop-down menu.)

Syntax: **copy xmodem flash < unix | pc >**

For example, to download a software file from a PC:

1. To reduce the download time, you may want to increase the baud rate in your terminal emulator and in the switch to a value such as 57600 bits per second. (The baud rate must be the same in both devices.) For example, to change the baud rate in the switch to 57600, execute this command:

   ```
   ProCurve(config)# console baud-rate 57600
   ```

   (If you use this option, be sure to set your terminal emulator to the same baud rate.)

2. Execute the following command in the CLI:

   ```
   ProCurve # copy xmodem flash primary
   The primary OS image will be deleted. continue [y/n]? Y
   Press 'enter' and start XMODEM on your host . . .
   ```

3. Execute the terminal emulator commands to begin the Xmodem transfer. The download can take several minutes, depending on the baud rate used in the transfer.

4. Reboot the switch.

   After the switch reboots, it displays the CLI or Main Menu, depending on the **Logon Default** setting last configured in the menu's Switch Setup screen.

5. Use the following command to confirm that the software downloaded correctly:

   ```
   ProCurve> show system
   ```

   Check the **Firmware revision** line to verify that the switch downloaded the new software.

6. If you increased the baud rate on the switch (step 1), use the same command to return it to its previous setting. (HP recommends a baud rate of 9600 bits per second for most applications.) Remember to return your terminal emulator to the same baud rate as the switch.

Saving Configurations While Using the CLI

The switch operates with two configuration files:

- **Running-Config File:** Exists in volatile memory and controls switch operation. Rebooting the switch erases the current running-config file and replaces it with an exact copy of the current startup-config file. To save a configuration change, you must save the running configuration to the startup-config file.

- **Startup-Config File:** Exists in flash (non-volatile) memory and preserves the most recently-saved configuration as the "permanent" configuration. When the switch reboots for any reason, an exact copy of the current startup-config file becomes the new running-config file in volatile memory.

When you use the CLI to make a configuration change, the switch places the change in the running-config file. If you want to preserve the change across reboots, you must save the change to the startup-config file. Otherwise, the next time the switch reboots, the change will be lost. There are two ways to save configuration changes while using the CLI:

- Execute **write memory** from the Manager, Global, or Context configuration level.
- When exiting from the CLI to the Main Menu, press **[Y]** (for Yes) when you see the "Do you want to save current configuration [y/n]?" prompt.

Software Index for ProCurve Networking Products

Software Letter	ProCurve Networking Products
C	1600M, 2400M, 2424M, 4000M, and 8000M
CY	Switch 8100fl Series (8108fl and 8116fl)
E	Switch 5300xl Series (5304xl, 5308xl, 5348xl, and 5372xl)
F	Switch 2500 Series (2512 and 2524), Switch 2312, and Switch 2324
G	Switch 4100gl Series (4104gl, 4108gl, and 4148gl)
H	Switch 2600 Series, Switch 2600-PWR Series: H.07.81 and earlier, or H.08.55 and greater, Switch 2600-8-PWR requires H.08.80 or greater. Switch 6108: H.07.xx and earlier
I	Switch 2800 Series (2824 and 2848)
J	Secure Router 7000dl Series (7102dl and 7203dl)
K	Switch 3500yl Series (3500yl-24G-PWR and 3500yl-48G-PWR), Switch 6200yl-24G, and 5400zl Series (5406zl, 5406zl-48G, 5412zl, and 5412zl-96G) and Switch 8212zl.
L	Switch 4200vl Series (4204vl, 4208vl, 4202vl-72, and 4202vl-48G)
M	Switch 3400cl Series (3400-24G and 3400-48G): M.08.51 though M.08.97, or M.10.01 and greater; Series 6400cl (6400cl-6XG CX4, and 6410cl-6XG X2): M.08.51 though M.08.95, or M.08.99 to M.08.100 and greater.
N	Switch 2810 Series (2810-24G and 2810-48G)
PA/PB	Switch 1800 Series (Switch 1800-8G – PA.xx; Switch 1800-24G – PB.xx)
Q	Switch 2510 (2510-48)
R	Switch 2610 Series (2610-24; 2610-48; 2610-24-PWR; 2610-24/12PWR; 2610-48-PWR)
T	Switch 2900 Series (2900-24G, and 2900-48G)
U	Switch 2510-48
VA/VB	Switch 1700 Series (Switch 1700-8 - VA and 1700-24 - VB)
WA	ProCurve Access Point 530
WS	ProCurve Wireless Edge Services xl Module and the ProCurve Redundant Wireless Services xl Module
WT	ProCurve Wireless Edge Services zl Module and the ProCurve Redundant Wireless Services zl Module

Software Letter	ProCurve Networking Products
numeric	Switch 9408sl, Switch 9300 Series (9304M, 9308M, and 9315M), Switch 6208M-SX and Switch 6308M-SX (Uses software version number only; no alphabetic prefix. For example 07.6.04.)

OS/Web/Java Compatibility Table

The switch web agent supports the following combinations of OS browsers and Java Virtual Machines:

Operating System	Internet Explorer	Java
Windows NT 4.0 SP6a	5.00, 5.01 5.01, SP1 6.0, SP1	Sun Java 2 Runtime Environment: – Version 1.3.1.12 – Version 1.4.2.05
Windows 2000 Pro SP4	5.05, SP2 6.0, SP1	
Windows XP Pro SP2	6.0, SP1	Sun Java 2 Runtime Environment: – Version 1.5.0.02
Windows Server SE 2003 SP1	6.0, SP1	

Enforcing Switch Security

ProCurve switches are designed as "plug and play" devices, allowing quick and easy installation in your network. However, when preparing the switch for network operation, ProCurve strongly recommends that you enforce a security policy to help ensure that the ease in getting started is not used by unauthorized persons as an opportunity for access and possible malicious actions. Since security incidents can originate with sources inside as well as outside of an organization, your switch and network access security provisions must protect against internal and external threats while preserving the necessary network access for authorized clients and uses.

This section provides an overview of switch management and network access security features and applications. *However, the features and applications supported by your switch depend on your particular switch model.* For information on specific features supported, refer to the software manuals provided for your switch model.

Caution:

In its default configuration, the switch is open to unauthorized access of various types. ProCurve recommends that you review this section to help ensure that you recognize the potential for unauthorized switch and network access and are aware of the features available to help prevent such access.

Switch Management Access Security

This section outlines provisions for protecting access to the switch's status information configuration settings. For more detailed information on these features, refer to the indicated manuals.

Default Settings Affecting Security

In the default configuration, switch management access is available through the following methods:

- Telnet

- Web-browser interface (including the ability to launch Telnet access)

- SNMP access

- Front-Panel access (serial port access to the console, plus resets and clearing the password(s) or current configuration)

It is important to evaluate the level of management access vulnerability existing in your network and take steps to ensure that all reasonable security precautions are in place. This includes both configurable security options and physical access to the switch hardware.

Local Manager Password

In the default configuration, there is no password protection. Configuring a local Manager password is a fundamental step in reducing the possibility of unauthorized access through the switch's web browser and console (CLI and Menu) interfaces. The Manager password can easily be set using the CLI **password manager** command, the Menu interface **Console Passwords** option, or the password options under the **Security** tab in the web browser interface.

Inbound Telnet Access and Web Browser Access

The default remote management protocols enabled on the switch, such as Telnet or HTTP, are plain text protocols, which transfer passwords in open or plain text that is easily captured. To reduce the chances of unauthorized users capturing your passwords, secure and encrypted protocols such as SSH and SSL must be used for remote access. This enables you to employ increased access security while still retaining remote client access.

■ SSHv2 provides Telnet-like connections through encrypted and authenticated transactions

■ SSLv3/TLSv1 provides remote web browser access to the switch via encrypted paths between the switch and management station clients capable of SSL/TLS operation.

Also, access security on the switch is incomplete without disabling Telnet and the standard web browser access.Among the methods for blocking unauthorized access attempts using Telnet or the Web browser are the following two commands:

■ **no telnet-server**: This CLI command blocks inbound Telnet access.

■ **no web-management**: This CLI command prevents use of the web browser interface through http (port 80) server access.

If you choose not to disable Telnet and web browser access, you may want to consider using RADIUS accounting to maintain a record of password-protected access to the switch.

Secure File Transfers

Secure Copy and SFTP provide a secure alternative to TFTP and auto-TFTP for transferring sensitive information such as configuration files and log information between the switch and other devices.

SNMP Access (Simple Network Management Protocol)

In the default configuration, the switch is open to access by management stations running SNMP management applications capable of viewing or changing usernames, passwords, configuration, and status data in the switch's MIB (Management Information Base). Thus, controlling SNMP access to the switch and preventing unauthorized SNMP access should be a key element of your network security strategy.

General SNMP Access to the Switch. The switch supports SNMP versions 1, 2c, and 3, including SNMP community and trap configuration. The default configuration supports versions 1 and 2c compatibility, which uses plain text and does not provide security options. ProCurve recommends that you enable SNMP version 3 for improved security. SNMPv3 includes the ability to configure restricted access and to block all non-version 3 messages (which blocks version 1 and 2c unprotected operation). SNMPv3 security options include:

- configuring device communities as a means for excluding management access by unauthorized stations

- configuring for access authentication and privacy

- reporting events to the switch CLI and to SNMP trap receivers

- restricting non-SNMPv3 agents to either read-only access or no access

- co-existing with SNMPv1 and v2c if necessary

SNMP Access to the Switch's Local Username and Password Authentication MIB Objects. A management station running an SNMP networked device management application such as ProCurve Manager Plus (PCM+) or HP OpenView can access the switch's management information base (MIB) for write access to the switch's local username and password configuration. In earlier software versions, SNMP access to the switch's local authentication configuration (hpSwitchAuth) MIB objects was not allowed. However, beginning with software release U.11.04, the switch's default configuration allows SNMP access to the local username and password MIB objects in hpSwitchAuth. If SNMP access to these MIB objects is considered a security risk in your network, then you should implement the following security precautions when downloading and booting from software release U.11.04 or greater:

1. If SNMP write access to the switch's local username and password authentication configuration (hpSwitchAuth) MIB (described above is not desirable for your network, then immediately after downloading and booting from the U.11.04 or greater software for the first time, use the following CLI command to disable this feature:

   snmp-server mib hpswitchauthmib excluded

Note on SNMP Access to Local Authentication MIB Objects

Downloading and booting U.11.04 or later software versions for the first time enables SNMP access to the switch's local authentication configuration MIB objects (the default action). If SNMPv3 and other security safeguards are not in place, the local username and password MIB objects are exposed to unprotected SNMP access and you should use the preceding command to disable this access.

2. If you choose to leave the local authentication configuration MIB objects accessible, then you should do the following to help ensure that unauthorized workstations cannot use SNMP tools to change the settings:

   • Configure SNMP version 3 management and access security on the switch.

   • Disable SNMP version 2c on the switch.

Front-Panel Access and Physical Security

Physical access to the switch allows the following:

■ use of the console serial port (CLI and Menu interface) for viewing and changing the current configuration and for reading status, statistics, and log messages.

■ use of the switch's Clear and Reset buttons for these actions:

   • clearing (removing) local password protection

   • rebooting the switch

   • restoring the switch to the factory default configuration (and erasing any non-default configuration settings)

Keeping the switch in a locked wiring closet or other secure space helps to prevent unauthorized physical access. As additional precautions, you can do the following:

■ Disable or re-enable the password-clearing function of the Clear button.

■ Configure the Clear button to reboot the switch after clearing any local usernames and passwords.

■ Modify the operation of the Reset+Clear button combination so that the switch reboots, but does not restore the switch's factory default settings.

■ Disable or re-enable password recovery.

Other Provisions for Management Access Security

Authorized IP Managers. This feature uses IP addresses and masks to determine whether to allow management access to the switch through the network, and covers access through the following:

■   Telnet and other terminal emulation applications

■   The switch's Web browser interface

■   SNMP (with a correct community name)

Secure Management VLAN. This feature creates an isolated network for managing the ProCurve switches that offer this feature. When a secure management VLAN is enabled, CLI, Menu interface, and web browser interface access is restricted to ports configured as members of the VLAN.

Network Security Features

This section outlines provisions for protecting access through the switch to the network. For more detailed information on these features, refer to the indicated manuals.

Web and MAC Authentication

These options are designed for application on the edge of a network to provide port-based security measures for protecting private networks and the switch itself from unauthorized access. Because neither method requires clients to run any special supplicant software, both are suitable for legacy systems and temporary access situations where introducing supplicant software is not an attractive option. Both methods rely on using a RADIUS server for authentication. This simplifies access security management by allowing you to control access from a master database in a single server. It also means the same credentials can be used for authentication, regardless of which switch or switch port is the current access point into the LAN. Web authentication uses a web page login to authenticate users for access to the network. MAC authentication grants access to a secure network by authenticating device MAC address for access to the network.

Secure Shell (SSH)

SSH provides Telnet-like functions through encrypted, authenticated transactions of the following types:

■   **client public-key authentication:** uses one or more public keys (from clients) that must be stored on the switch. Only a client with a private key that matches a stored public key can gain access to the switch.

■ **switch SSH and user password authentication:** this option is a subset of the client public-key authentication, and is used if the switch has SSH enabled without a login access configured to authenticate the client's key. In this case, the switch authenticates itself to clients, and users on SSH clients then authenticate themselves to the switch by providing passwords stored on a RADIUS or TACACS+ server, or locally on the switch.

■ **secure copy (SC) and secure FTP (SFTP):** By opening a secure, encrypted SSH session, you can take advantage of SC and SFTP to provide a secure alternative to TFTP for transferring sensitive switch information.

Secure Socket Layer (SSLv3/TLSv1)

This feature includes use of Transport Layer Security (TLSv1) to provide remote web access to the switch via authenticated transactions and encrypted paths between the switch and management station clients capable of SSL/TLS operation. The authenticated type includes server certificate authentication with user password authentication.

Enhancements

Unless otherwise noted, each new release includes the features added in all previous releases. Enhancements are listed in chronological order, oldest to newest software release.

Release U.11.04 Enhancements

No new enhancements. Initial Release.

Software Fixes in Release U.11.04

Software fixes are listed in chronological order, oldest to newest.

Unless otherwise noted, each new release includes the software fixes added in all previous releases.

Release U.11.04 was the first software release for the ProCurve Series 2610 Series Switches.

Release U.11.04

No Problems Resolved in Release U.11.04. Initial Release.